***** PUBLIC VERSION *****

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant.	Case No. 1:20-cr-00143 Honorable T.S. Ellis, III Sentencing: April 1, 2022

REPLY TO THE GOVERNMENT'S RESPONSE TO MOTION FOR NEW TRIAL AND TO RECONSIDER MOTIONS TO COMPEL AND MOTIONS TO SUPPRESS

Mr. Zackary Sanders, through undersigned counsel, respectfully submits this Reply to the Government's Opposition to the Motion for New Trial and to Reconsider Motions to Compel and Motions to Suppress. In its Response (ECF No. 593), the government admits for the first time after two years of litigation and numerous discovery requests, motions to compel, and motions to suppress a game-changing fact it has been aware of all along: that the foreign law enforcement agency (FLA) that seized [redacted] is not the [redacted], as both the defense and the Court have believed for years. And while the government fails to grapple honestly with the ramifications of this disclosure, it is obvious both from logic and the government's representations in its Response that the disclosure strips the FLA tip recounted in the Affidavit of any indicia of reliability. Because a bare-boned tip that originated from an unknown source with no indicia of reliability cannot possibly support probable cause, the Court should order a new trial and suppression of the physical evidence in this case.[1]

[1] The government suggests, without truly arguing, that the Court cannot grant a new trial based on the newly discovered evidence because it pertains to the government's violation of the Fourth

The government's Response makes five things clear. First, the FLA discussed in Paragraph 25 of the Affidavit was not the FLA that "de-anonymized" Mr. Sanders's IP address.[2] Second, the government continues falsely to equate visiting the website a single time with accessing content on the site, notwithstanding the plain meaning of the FLA tip and the FBI and HSI's numerous representations to the contrary, including the representation in Paragraph 23 of the Affidavit. Third, the U.S., [redacted], and other international partners were jointly investigating [redacted] but the government claims only that the narrow, later investigation into Mr. Sanders's IP address was "independent." Fourth, given the FBI's possession of a searchable copy of [redacted] all along, the FBI had custody of exculpatory evidence regarding Mr. Sanders's IP address prior to the execution of the search warrant, including that the IP address was never used to register an account on [redacted] or login to [redacted] (two prerequisite steps to being able to access *any* illegal content on [redacted] Fifth, a Network Investigative Technique (NIT) must have been deployed to generate so many IP address leads.

Mr. Sanders's motion should be considered timely because the additional materials—which reflect information the government has had in its possession all along—were not available to the defense when previously litigating Mr. Sanders's motions to compel and motions to suppress. The government has opposed disclosure at every opportunity. The reason why the government fought so hard is obvious—the information that has finally come to light (and which

---

Amendment instead of the trial evidence itself. The government's position has no basis in law or logic, and it cites no supporting authority for this proposition. Because the newly discovered evidence requires suppression under the Fourth Amendment, the *United States v. Chavis*, 880 F.2d, 788, 793 (4th Cir.1989) factors are all plainly met.

[2] The government's concession that an FLA "de-anonymized" Mr. Sanders's IP address is itself revealing, as it represents the first time the government has admitted that an FLA deployed a technique that would force a computer to reveal its IP address, thus necessarily "interfering" with the computer.

the government knew all along) makes clear that the tip had no reliability and the Affidavit was materially misleading. It now seeks to hide behind deadlines to avoid the impact of those disclosures. The Court should not reward such procedural chicanery.

In light of the new materials and the entire record, this Court should grant Mr. Sanders's previously filed Motions to Compel, order a hearing pursuant to *Franks v. Delaware,* 438 U.S. 154 (1978), suppress all evidence obtained pursuant to the invalid search warrant, and order a new trial pursuant to Fed. R. Crim. P. 33. Time is running out for this Court to take corrective action based on newly available information that the government concealed. But the defense anticipates that more evidence will come to light about this operation, which will further contradict both the Affidavit and the government's representations about this operation and the identification of Mr. Sanders's IP address. Mr. Sanders should not be sentenced based on information obtained through the illegal seizure of his IP address and the illegal search of his family's home.

DISCUSSION

I. The government's Response makes clear that the FLA in Paragraph 25 of the Affidavit was not the FLA that "de-anonymized" Mr. Sanders's IP address.

In its Response, the government finally confirms what the defense learned only due to its own investigation: that "[t]he agency that seized the server is not the FLA described in paragraphs 22 through 26 of the Affidavit that conducted the investigation that led to the information in the tip."[3] ECF No. 593 at 2. This admission comes after two years of litigation, during which the defense filed numerous requests and motions to compel regarding, *inter alia*, precisely this issue.

[3] The government fails to represent how or when it learned the fact that this other agency seized the website. The government's failure to explain its knowledge only underscores the government's persistent willingness in this case to mislead the defense and the Court in asserting that "the tip" was only the three documents the government has proffered and that there was no further relevant information in its possession, custody, or control regarding the seizure of Mr. Sanders's IP address. This is part of a larger pattern in this case of the government withholding critical information,

The question now is what this admission means for the reliability of the Affidavit (ECF No. 254-3) and, in particular, the reliability of the FLA tip.

The government refuses to answer the central question underlying Mr. Sanders's motion: which FLA deployed the de-anonymizing technique that identified Mr. Sanders's IP address as having accessed [redacted] on May 23, 2019, at 02:06:48 UTC. The government once again declines to say *what did happen—i.e.*, which country obtained Mr. Sanders's IP address through the use of an NIT or an alternative method (however unlikely and inaccurate)—but chooses instead to blast the defense for not having already "proven" that the [redacted] was not the country that deployed the de-anonymizing technique.

The government's omissions on which FLA de-anonymized the IP address speak volumes. Continuing its pattern of creative wordsmithing and non-denial denials, the government ties itself in knots to differentiate its actions in *Kiezjo*, where evidence shows that a second FLA seized *and* de-anonymized the target user's IP address, from this case. As an initial matter, the government fails to inform the Court that it originally suggested to the defense that *Kiezjo* was not even from the same operation,[4] a false claim that it has abandoned here. More importantly, it states "[b]ased on the order [in *United States v. Vincent Kiejzo*, Case No. 20-cr-40036-TSH (D. Mass.)], it appears that the defendant in that case asked whether the country that seized a server containing two websites was the same FLA that provided the tip in his case, and the government advised that it was not. Nowhere does the government state that the country that seized the server also de-

---

including by artificially defining what constitutes "the investigation" into Mr. Sanders and "the tip" as it relates to Mr. Sanders. It is only through its incorrect view of what constitutes *Brady* material that the government is even able to claim—in that incorrect sense—that it has complied with its discovery obligations.

[4] 2022/03/04 Government Email (ECF No. 588-3) at 2-3 (AUSA Clayman representing that *Kiejzo* "does not appear to involve the same tip as the one related to [Mr. Sanders]").

anonymized the defendant's IP address and told the FLA." ECF No. 593 at n.1. In other words, the government is expressly *declining* to represent that it was the [redacted] that "de-anonymized" Mr. Sanders's IP address.

Paragraph 25 of the Affidavit clearly suggests that the [redacted] deployed the technique to de-anonymize Mr. Sanders's IP address in the first place. Although the newly discovered evidence the defense has uncovered suggests that this is not true, the government's Response does not grapple with that central question. Instead, it avoids answering the question by using vague language and improperly putting the burden to prove what happened on the defense:

- Noting that the [redacted] "advised that it *obtained this information* through its own lawful, independent investigation without interfering with any computer in the United States." ECF No. 593 at 1 (emphasis added).

- Describing defense contention in *Kiejzo* that an unnamed FLA—not the [redacted]—both seized the server and deployed the de-anonymizing technique not as incorrect but as "unsupported." *Id.* at 3.

- Stating that the government "confirm[ed] that the statements in the Affidavit about his IP address *came from the same reliable FLA* that has been the subject of his prior motions and that this FLA advised that it *collected this data* through an independent and lawful investigation." *Id.* at 8 (emphases added).

- Stating "the cherry-picked, generic sentence from the plea agreement—'Law enforcement infiltrated this dark web website and determined that the defendant had utilized the website'—in no way proves that an unknown country obtained the information in the FLA's tip. . . . And even assuming these documents provide some support for his efforts to conflate the seizure of a server with the FLA's independent investigation and tip—which they do not—the defendant provides no support for the many other inferences required to make this claim material to a challenge to the Affidavit." *Id.* at 7.

The issue is not whether the [redacted] "collected [Mr. Sanders's IP address] through an independent and lawful investigation," *id.* at 8, as the government would have it. If the [redacted] "collected" or "obtained" Mr. Sanders's IP address' information *from the FLA that deployed the de-anonymizing technique*, then the government's representations about the reliability and legality

of the [redacted]'s actions—including those in Paragraph 25—are beside the point. Indeed, nowhere does the government represent anything inconsistent with the view that the [redacted] collected Mr. Sanders's IP address information not from its own use of a de-anonymizing technique but rather from the second FLA. The reason the government carefully avoids ever representing that the FLA described in Paragraph 25 was the FLA that "de-anonymized" Mr. Sanders's IP address is for the obvious reason that it was not.

The government's new admission that another FLA in fact had control of the website is a game-changing factual development.[5] The entire point of Paragraph 25 of the Affidavit is to provide the reader (whether it be the Magistrate Judge or this Court) with comfort that Mr. Sanders's IP address was obtained in both a reliable and legal manner. In light of the government's admission that another FLA seized the website—as well as the government's conspicuous failure to represent that it was the [redacted] that deployed the de-anonymizing technique—neither the Magistrate Judge nor this Court had any evidence regarding either the reliability or legality of the process that resulted in the tip. This pivotal (and obvious) point is the furthest thing from being "untethered from any unifying argument or principle." ECF No. 593 at 4. To the contrary, given that the reliability of the tip is the central Fourth Amendment issue here, and that the tip no longer has any indicia of reliability, the government's new admission requires a new trial, a *Franks* hearing, and suppression of the physical evidence. At a minimum the Court should grant Mr.

[5] The fact that the government has made this admission for the first time now and yet spends much of its pleading complaining about the defense's purportedly late filings reflects unbridled hypocrisy and is part and parcel of its concerted effort to use erroneous procedural objections to obstruct the search for truth in this case. Furthermore, though the government claims it has no duty to correct the defense's incorrect beliefs (even ones it has fostered), ECF No. 593 at 9, n.3, the fact is that the Court has been misled many times as well, ECF No. 586 at 11 (noting instances where Court was acting under the reasonable belief that the seizing FLA and the FLA referred to in Paragraphs 22 through 26 of the Affidavit were one and the same).

Sanders's previously filed motions to compel and require the government to disclose what actually happened, rather than accept its carefully worded statements that obscure the facts.

II. The government continues falsely to equate *visiting* the website a single time with *accessing content* on the site notwithstanding the plain language of the FLA tip and the FBI and HSI's numerous representations to the contrary.

In its Response, the government once again blatantly misrepresents the meaning of the FLA's tip. The government states that "the investigation of the defendant began when the [FBI] received a tip from a[n] [FLA] that his [IP] address was used on May 23, 2019 to access 'child sexual abuse and exploitation material' *on a hidden service on The Onion Router network ('Tor,' also known as the 'dark web')* dedicated to depictions of violent child sexual abuse ('Target Website')." ECF No. 593 at 1 (emphasis added); *see also id.* at 1-2 (stating that "the Target Website was seized by a foreign law enforcement agency in June 2019, after the defendant's IP address was used to access child sexual abuse material on the site.").

The FLA tip did not say this. To the contrary, it was the government (and, purportedly, Special Agent Ford[6]) who added the language "via a website" to the tip; the tip itself conveyed only that the IP user accessed a website, on a single date (May 23, 2019), at a single time (02:06:48 UTC). Indeed, the prosecutors in the *Kiejzo* case—unlike the prosecutors here—have complied with their duty of candor to the Court on this issue (and others), admitting that "access[ing]" the website and "logg[ing] in" to the website are not the same and that "[t]he United States is not in possession of … information that [the defendant] in *Kiejzo*] in particular created an account" and that "[t]he only information that [the U.S.] was provided was that the IP address that was linked to his house accessed these websites." *Kiejzo* Transcript (ECF No. 588-1) at 41; *see also id.* at 43

[6] Based on, *inter alia*, the affidavits from the other cases arising from the same operation, it is abundantly clear that Special Agent Ford actually wrote very little, if any, of his own Affidavit.

(similar). As the government has always known, and as the other cases located by the defense definitively establish, the [redacted] considers *the entire website* to be "child sexual abuse and exploitation material," and was describing the website as opposed to any content. *Compare* Intel Log (ECF No. 253-1) *with* FLA Report (ECF No. 253-3) (using same language to describe the website as a whole) and Affidavit (ECF No. 254-3) at ¶ 24 (same); *see also* Case Comparison (ECF No. 588-4). The government's rehashing of this discredited version of the tip is nothing short of an attempt to (continue to) knowingly mislead this Court.

III. The government's Response admits that the U.S. and the [redacted] were jointly investigating [redacted] and claims only that the subsequent, narrow investigation into Mr. Sanders's IP address was purportedly "independent."

The government's response makes clear that the U.S., [redacted], and other foreign law enforcement agencies were jointly investigating [redacted] The government now claims only that the subsequent, narrow "investigation" by the [redacted] into Mr. Sanders's IP address was even purportedly "independent." Understood correctly and in the larger context, the claimed independence of the [redacted]'s investigation, into Mr. Sanders's IP address alone, provides no basis to avoid the application of the joint venture doctrine and the Fourth Amendment.

Contrary to what the Affidavit in this case suggested to the Magistrate Judge, and what the government has represented to this Court, U.S. law enforcement's investigation into [redacted] and other Tor websites related to [redacted] had begun by January 2017, *see* 2017/01/13 FD-302 (ECF No. 586-17) (documenting the opening of the FBI's preliminary investigation of [redacted] *see also* 2017/01/13 FD-340 (ECF No. 586-18) (documenting FBI's collection of [redacted] screenshots), more than two years before Mr. Sanders's IP address allegedly visited [redacted] on a single date, at a single time (May 23, 2019, 02:06:48 UTC). That investigation was a "joint"

investigation, conducted alongside, at minimum, [redacted] law enforcement agencies.[7, 8]

As part of that investigation, U.S. law enforcement obtained passwords, encryption keys, and signature keys, ECF No. 392-1,[9] that allow the owner to take control of Tor websites, including [redacted] and identify visitors to those websites by seizing their IP addresses. Additional material that has become publicly available earlier this month has revealed that Operation H (another name for what appears to be [redacted] and/or [redacted])[10] included more than the [redacted], but also included at least [redacted]

[7] The other cases demonstrate that HSI also had a significant role in this operation. Whether federal law enforcement was acting through the FBI or HSI or both, the joint venture analysis is the same.

[8] *See, e.g.,* Tyler Walker Report to Crown Counsel (ECF No. 392-1) (describing "[redacted]," as well as assistance from [redacted] and the [redacted] *see also* Tyler Walker Sentencing Transcript (ECF No. 392-2) at 3 (demonstrating that the Walker investigation included an investigation into his activities in creating [redacted] News Story 1 (ECF No. 476-1) (describing "[redacted]" that included "[redacted]" and "[redacted] News Story 2 (ECF No. 476-2) (discussing Tyler Walker's arrest [redacted]" into "[redacted] News Story 3 (ECF No. 476-3) (similar).

[9] This information was obtained from, *inter alia*, Benjamin Faulkner and Patrick Falte, *United States v. Benjamin Alexander Faulkner and Patrick Dane Falte*, Case No. 3:17-CR-00049-JAG (E.D. Va., Oct. 4, 2016) (Criminal Complaint); *see also United States v. Patrick Dane Falte, Benjamin Alexander Faulkner, Andrew Ryan Leslie, and Brett Allen Bedusek*, Case No. 3:17-CR-00044 (M.D. Tn., Mar. 29, 2017) (Indictment), and Mr. Walker, ECF No. 392-2 at 9 (noting that Mr. Walker [redacted]).

[10] *See, e.g.,* Intel Log (ECF No. 253-1) (referencing "[redacted]"), *see also* FLA Report (ECF No. 253-3) (describing five files shared on [redacted] and describing report as being disseminated to "[i]nternational partners in receipt of [redacted] intelligence"); *see also* FLA Inspection Report (ECF No. 138-1) ([redacted]").

[redacted]. Notably, in its opposition, the government does not deny that Operation H refers to [redacted] and/or [redacted]. ECF No. 593 at 6 (denying that the Operation H press releases "have any bearing on the reliability of the FLA's tip or the accuracy of the Affidavit," without explaining how that is so or denying the connection between Operation H and this case). The years-long joint nature of this operation cannot be overcome by the representation that the government's investigation into Mr. Sanders's IP address was "independent," for it necessarily would have relied on information obtained as part of a joint venture. This joint venture evidence requires at a minimum additional discovery into the actions of FLAs to determine whether their conduct violated the Fourth Amendment.

IV. The government's attempt to discount its possession of the [redacted] website is utterly unconvincing.

The government's treatment of the Complaint (ECF No. 588-2) in [redacted] makes clear that the FBI possessed exculpatory evidence regarding Mr. Sanders's IP address's activity that the FBI declined to include in the Affidavit and that the government withheld from the defense. In its Response, the government characterized the [redacted] Complaint (ECF No. 588-2) as "an out-of-district complaint filed in January 2020, which describes what appear to be archived postings on a Tor site obtained after a defendant provided, among other information that may not be disclosed in the complaint, his username and password to the site." ECF No. 593 at 9.

In its Response, the government finally acknowledges—after two years of litigation—that it has been in possession of a full, searchable copy of [redacted] since at least the time it submitted the Affidavit. ECF No. 593 at 9. The government then downplays the significance of this resource, however, arguing that it has not yet been able to "investigate [Mr. Sanders's] criminal activity" on

[redacted] because it has no evidence of his username or password. *Id.* at 9. The government also stated that "if [Mr. Sanders] wishes to provide his true username and password," only then would the government be able to see what activity Mr. Sanders engaged in on [redacted] *Id.* at 9.

The government's admission that it possessed a searchable copy of [redacted] is significant, as it is now clear that the FBI could have (and likely did) investigate site activity (or lack thereof) on May 23, 2019 at 02:06:48 UTC, regardless of whether or not it had Mr. Sanders's username. This investigation would have shown that Mr. Sanders never registered an account, logged into, or attempted to or did access illegal content on [redacted] and that the FBI knew that there was not enough for probable cause. The lack of any incriminating evidence of any user who accessed the site on May 23, 2019, at 02:06:48 UTC is a material omission from the Affidavit that would have further undermined the existence of probable case. The government's failure to include that exculpatory evidence in the Affidavit requires suppression. *Franks,* 438 U.S. at 156 (finding an omission material if it is "necessary to the [neutral and disinterested magistrate's] finding of probable cause"); *see also United States v. Wharton*, 840 F.3d 163, 168-169 (4th Cir. 2016) (finding an omitted fact "is material if it is necessary to the . . . finding of probable cause;" in order words, if "its inclusion in the affidavit would defeat probable cause"); *Miller v. Prince George's Cty., MD*, 475 F.3d 621, 629 (4th Cir. 2007) (explaining that "selectively includ[ing] information bolstering probable cause, while omitting information that did not . . . can mislead a magistrate by reporting less than the total story, thereby manipulating the inferences a magistrate will draw").

Finally, the government fails entirely to respond to Mr. Sanders's argument that if law enforcement needs a username to investigate an IP user's activity, and it did not have that here, then there is no possibility that the FLA tip meant that the IP user accessed *content* on the site.

ECF Nos. 253, 467, 588. This is yet another example of the government attempting to have it both ways and abandoning its credibility in the process.

V. The government fails to respond to the overwhelming evidence now in the record that an NIT was used to de-anonymize thousands of IP addresses, including Mr. Sanders's IP address.

While the government has been careful to claim that the statements in the Affidavit about Mr. Sanders's IP address came from the [redacted], and that this information was collected lawfully,[11] ECF No. 593 at 8, the government still has not actually identified the country that deployed the method to de-anonymize Mr. Sanders's IP address or identified what method was actually used. Regardless of the government's intransigence, the evidence now in the record points overwhelmingly to an NIT being used. *See, e.g.,* ECF Nos. 586-23 to 586-38 (FBI FD-1057s

[11] [redacted]

reflecting that form electronic communications (ECs) were used and revealing the large-scale and boiler-plate nature of this operation).[12]

The use of form affidavits (and other form documents, including FBI ECs) corroborates that an NIT was used to identify IP addresses that purportedly visited [redacted] and other Tor websites that U.S. law enforcement was jointly investigating with other FLAs. Indeed, the NIT generated so many leads that the FBI and HSI had to rely on form documents to handle the enormous volume of so many simultaneous investigations.[13]

While dismissing the defense's evidence as comprising "'conspiratorial' theories" and "claims based on 'a stack of hypotheticals,'" ECF No. 593 at 4, the government fails to rebut or address evidence that an NIT was used. The government's blanket unsupported denial is not new and should be scrutinized against the backdrop of its earlier actions. The government previously dismissed as hypothetical the defense's arguments that: (a) contrary to what the Affidavit represented, [redacted] homepage did not allude to child pornography but was completely non-

[12] If an NIT was not used, the only other viable method is passive traffic analysis, which should be considered as producing a false positive if based only on a single identification, but such an approach would not have produced the number of IP addresses that were produced as part of this operation. *See, e.g.,* Murdoch Decl. (ECF No. 467-2); Clayton Decl. (ECF No. 256-8). Moreover, the kind of warrants the [redacted] obtained—[redacted]—indicates that it had to be an NIT. Had the [redacted] used traffic analysis, the proper warrant would have been a [redacted] warrant. *See supra* at n.11.

[13] *Compare* Affidavit (ECF No. 254-3) *with* ECF Nos. 586-2 (*Kiejzo* Objection), 586-4 (*Clark* Complaint), 588-2 (*Stauffer* Complaint), 586-6 (*Bateman* Motion), 586-7 (*Lawson* Plea Agreement), ECF No. 586-9 (North Carolina Affidavit), 586-10 (Vermont Affidavit), ECF No. 586-11 (Missouri Affidavit), ECF No. 586-12 (Florida Affidavit), ECF No. 586-13 (Maine Affidavit), ECF No. 586-14 (New Hampshire Affidavit), ECF No. 586-15 (Michigan Affidavit), ECF No. 586-21 (*Kidder* Complaint), ECF No. 586-22 (*Clemence* Complaint), ECF No. 588-6 (*Stauffer* Statement of Facts). *See also infra* at 19-20.

descript;[14] (b) that the FBI had no evidence that Mr. Sanders had ever registered an account or logged in to [redacted][15] (c) that the FBI had subpoenaed information not just about Mr. Sanders's IP address, but about a large number of IP addresses;[16] and (d) that this was an international operation that required the FBI to work closely with other law enforcement partners, as it had in all previous major operations to take down Tor websites that contained child pornography.[17] In *all* of these instances, the government selectively withheld information that turned out to exist and

---

[14] The government withheld for 224 days, until after the resolution of Mr. Sanders's motions to compel and to suppress, an exculpatory screenshot of [redacted] homepage, notwithstanding the defense's efforts to compel that screenshot and after repeatedly characterizing Mr. Sanders's requests for that screenshot as a "fishing expedition." *See* ECF No. 176 at 1-19; No. 176-1 (Homepage screenshot); *cf.* Gov't Opp'n (ECF No. 57) at 6 (arguing that Mr. Sanders's requests, including for the screenshot, were "nothing more than . . . an impermissible fishing expedition to find some hypothetical document or communication to support his otherwise unfounded theories," despite sitting on evidence that the government knew supported the defense's position); Gov't Opp'n (ECF No. 101) at 26 (noting that Mr. Sanders "asserts that the Affidavit misleadingly described the Target Website as dedicated to the . . . advertisement of child pornography, . . . the only basis he appears to have for his claim is . . . a post on the site stating that it was created to host images and videos of '18 (twinks) and younger," while in possession of the innocuous homepage all along, which did not advertise illegal content or even allude to it).

[15] *Compare* 2020/07/31 Tr. (ECF No. 255-1) at 33 ("MR. CLAYMAN: the face of the tip . . . says [Mr. Sanders] did go in, [he] did access illegal content") *with* Gov't Opp'n (ECF No. 593) at 2 (stating that law enforcement were unable to determine whether Mr. Sanders engaged in any activity on [redacted] because they did not associate any username with him, even though registering an account and logging in were necessary prerequisite steps to attempting to or actually accessing any child pornography on [redacted] whatsoever).

[16] *See, e.g.,* Memorandum in Support of Motion to Compel, or, in the Alternative, to Submit Material for *In Camera* Inspection (ECF No. 335) at 1-3 (explaining how the scope of the operation and the involvement of [redacted], which the government had tried to conceal, corroborates that an NIT and/or pen register/trap and trace device was used to identify IP addresses and then triage those IP addresses, just as the FBI had done in previous operations); November Subpoena (ECF No. 335-2) (revealing that the FBI sought subscriber information for 291 IP addresses associated with Cox, including the Sanders family's IP address).

[17] *See, e.g.,* 2017/01/13 FD-302 (ECF No. 586-17), 2017/01/13 FD-340 (ECF No. 586-18), Tyler Walker Report to Crown Counsel (ECF No. 392-1), Tyler Walker Sentencing Transcript (ECF No. 392-2 [redacted]).

that corroborated Mr. Sanders's arguments challenging the validity of the search warrant. As such, the Court should carefully scrutinize the government's representations here and should order the government to produce the relevant documentation, at minimum to the Court for *in camera* review.

VI. The additional materials were not available to the defense when previously litigating Mr. Sanders's motions to compel and motions to suppress.

The additional materials contain information that was in the government's possession, custody, or control all along. Because of the government's cramped view of its discovery obligations, however, the defense was only recently able to obtain these materials through its own independent investigation and then assess their significance in light of the record.

The government argues that the defense previously had all the information it shared in its Motion except the Operation H press releases. ECF No. 593 at 6. That is incorrect. First, the information from the *Kiejzo*, Case No. 20-cr-40036-TSH, and *United States v. Paul Bateman*, Case No. 1:20-cr-10012-IT (D. Mass, Dec. 27, 2021) cases (ECF Nos. 586-1, 2, 6), only became available after Mr. Sanders's trial had concluded. Second, the information from other cases that arose from the same operation (ECF Nos. 586-4, 5, 7, 9-16, 20-22, 45) was precisely the information that the defense has requested and moved to compel but was nevertheless denied. Third, the FBI ECs (ECF Nos. 586-3, 17-18, 23-38) were only made public on or about November 29, 2021, and January 31, 2022—again, after Mr. Sanders's trial had concluded. *See* 2022/01/31 FOIA Release Letter, attached as Ex. 4; 2021/11/29 FOIA Release Letter, attached as Ex. 5. Fourth, the Operation Plan (ECF No. 588-44) was disclosed *during* Mr. Sanders's trial, after the Court concluded that it was *Jencks* material of Special Agent Jeremy Obie. Finally, the "Operation H" press releases were published on March 1 and 2, 2022 (ECF Nos. 586-39 to 586-43).

The information contained in these five types of documents is precisely the kind of information that the defense requested of the government and moved to compel because it was

relevant to his motions to suppress, but that the government refused to provide and that the Court refused to order the government to disclose.[18] All of this information was in the government's possession, custody, or control all this time.

A. The *Kiejzo* and *Bateman* Disclosures

The information that the government disclosed in *Kiejzo*, Case No. 20-cr-40036-TSH, but failed to disclose in this case—that there was a third country involved in investigating [redacted] whose rule of law and reliability and are not addressed in the Affidavit—only became available

[18] *See, e.g.,* 2020/06/22 Discovery Letter (ECF No. 176-7) at 4, 6-8 (requesting, *inter alia*, "[i]nformation regarding the number of IP addresses that the FLA provided to the FBI prior to February 10, 2020, and how many of those IP addresses were ones that the FBI was unable to corroborate . . . as being used to engage in illegal activity;" "[a]ll information . . . that formed the basis of the government's assertion . . . that '[t]he defendant came to the government's attention after an investigation conducted by the [FBI] . . . and other law enforcement entities revealed that an individual accessed a website that advertises child pornography;'"; "[a]ll information that Special Agent Ford knew, or should have known, that the facts alleged in the FD-1057 form were insufficient to support a finding of probable cause;" and "[a]ll information, photographs, and documents tending to show that Special Agent Ford copied language in the affidavit . . . from an affidavit in another case"); 2021/01/22 Discovery Letter (ECF No. 241-3) at 3 (requesting, *inter alia*, "the template affidavit that Special Agent Ford relied on to draft the Affidavit in this case, and which FBI agents have relied on to draft affidavits in other cases related to [redacted] and [redacted]," which "would demonstrate that the allegations in [the] Affidavit were generic and not specific to Mr. Sanders; . . . that there was no effort to corroborate the FLA's tip; that this was a bulk operation that was meant to describe the activities of a large number of individuals . . . . ; and that there was no evidence of Mr. Sanders's activity on the website, as Paragraph 23 of the Affidavit clearly suggested there was;" "the numbers of IP addresses that the FLA provided to the FBI under i) [redacted] and ii) [redacted]; the number of IP addresses that the FBI sought search warrants for; and the number of searches that did not lead to child pornography charges being filed;" "additional reports relating to this Operation and its case developments"); *see also* 2020/05/08 Discovery Letter (ECF No. 176-5) (making initial discovery requests); 2020/06/08 Discovery Letter (ECF No. 176-6) (explaining why previously requested discovery was material and exculpatory); *see also* 2020/07/07 Discovery Letter (ECF No. 176-8) (noting that the limited documents the government had provided pertaining to the search warrant "cannot be the extent of items . . . that relate to the tip from the FLA, the FLA's reliability (or lack thereof), the target website and its server, the [NIT](s), the FBI's efforts to corroborate the FLA tip (or lack thereof), or Special Agent Ford's knowledge"). *See also* ECF No. 586-28 (FBI unable to corroborate that IP address accessed child pornography on target website).

with the release of the *Kiejzo* Transcript on the public docket on January 10, 2022. Although the government argues that the *Kiejzo* objection (ECF No. 596-2) was filed on October 18, 2021, that was after this Court had ruled on Mr. Sanders's motions to compel and motions to suppress and on the eve of trial. Subsequent developments in *Kiejzo* and *Bateman*, Case No. 1:20-cr-10012-IT, including the release of the *Kiejzo* Transcript (ECF No. 588-1) on January 10, 2022, and the filing of Mr. Bateman's Motion to Suppress on December 27, 2021 (ECF No. 586-6), occurred well after Mr. Sanders's trial.

B. Information about Cases Arising from the Same Operation

The defense was denied the type of information that would have given the defense access to cases arising from the same operation at an earlier point in time. The defense was unable to include the information in ECF Nos. 586-4, 5, 7, 9-16, 20-22, 45 prior to the resolution of his motions to compel and suppress because the government withheld this information and the defense was not aware of and unable to locate those cases.

While some of the additional documents from cases arising from the same investigation of Tor websites, including [redacted] appear to have been filed (and may have been unsealed) during a time when Mr. Sanders theoretically could have made use of them *if and only if* the defense had been aware of their existence (which the defense was not), without the information that the government possessed, the defense was limited in its ability to search court documents without knowing the addresses where related searches were executed or the identities or case numbers of individuals who were charged. The defense only became aware of the majority of these cases through Freedom of Information Act (FOIA) releases, and was subsequently able to locate additional cases based on materials released through FOIA. *See* Ex. 4 (2022/01/31 FOIA Release Letter); Ex. 5 (2021/11/29 FOIA Release Letter); *see infra* at 18. The government undoubtedly

has additional information material to Mr. Sanders's motions to compel and to suppress (and to the credibility of the affidavit) about other cases with the substantially same affidavit (*see, e.g.,* ECF No. 588-4) that arose from the same operation.

C. The FBI Electronic Communication Documents (FD-1057s, 302s, 340s)

The FBI EC documents (ECF Nos. 586-3, 17-18, 23-38) were only made public on or about November 29, 2021, and January 31, 2022 as a result of FOIA disclosures. *See* Ex. 4 (2022/01/31 FOIA Release Letter); Ex. 5 (2021/11/29 FOIA Release Letter). These FBI FD-1057s, 302s, and 340s further corroborate similarities between this operation and Pacifier (ECF No. 586-19), which also relied on form ECs and affidavits because of the many IP addresses the NIT generated.

D. The Operation Plan

The Operation Plan (ECF No. 588-5) was only disclosed to the defense during trial on October 25, 2021, over the government's objection after the Court made an *in camera* examination and determined that it "fit[] within the terms of the *Jencks* Act." 2021/10/25 Tr. at 44-46, 95-96. The Operation Plan was drafted by Special Agent Obie on February 6, 2020. ECF No. 588-5. It appears that the government withheld this Operation Plan precisely because—like Special Agent Ford's FD-1057 (ECF No. 253-4) at 2, Special Agent Obie's Affidavit in Support of a Criminal Complaint (ECF No. 4) at ¶ 9, and the government's opposition to a motion for revocation of detention (ECF No. 15 at 2)—it corroborated that the true meaning of the tip was merely that an Internet user had "accessed [redacted] using IP address 98.169.118.39, on May 23, 2019, at 02:06:48 UTC," contrary to what Paragraph 23 of the Affidavit represented.[19] ECF No. 588-5.

[19] *Compare* ECF Nos. 4, 15, 253-4, 588-5 (correctly stating that the tip meant that the Internet user had "accessed" a website called [redacted] not any illegal content via [redacted] *with* Affidavit (ECF No. 254-3) at ¶ 23 (incorrectly stating that the tip meant that "on May 23, 2019, a user of IP address 98.169.118.39 accessed online child sexual abuse and exploitation material via a website that the FLA named and described as the TARGET WEBSITE").

E. Operation H Information

The "Operation H" press releases were published in March 2022 (ECF Nos. 586-39 to 43).

VII. There are additional materials that the government continues to withhold that corroborate Mr. Sanders's arguments for suppression and contradict the Affidavit, the government's representations, and this Court's rulings.

The additional materials that the defense has been able to uncover that were unavailable during the litigation of Mr. Sanders's motions to compel and motions to suppress represent much more information that the government continues to withhold. Even in the past week, since Mr. Sanders filed his motion, his defense team has learned of two additional cases that stem from the same operation that led to the seizure of Mr. Sanders's IP address. *See United States v. Benjamin Shacar*, Case No. 3:21-CR-30028-MGM (D. Mass., Mar. 24, 2021) (Complaint) ("*Shacar* Complaint"), attached as Ex. 6; *see also United States v. Joshua White*, Case No. 3:21-CR-155-DJH (W.D. Ky., Jan. 28, 2022) (Affidavit in Support of Application for a Search Warrant) ("*White* Affidavit"), attached as Ex. 7; *compare* Ex. 7 (*White* Afifdavit) *with* Affidavit (ECF No. 254-3).

In *Shacar*, the true meaning of the FLA's tip is evident: the HSI agent understood that the tip meant merely that an IP address had been used to access a website, not to register an account, login, and view illegal content on the website. Ex. 6 (*Shacar* Complaint) at ¶ 8 ("There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE. . . . There is probable cause to believe that the user, SHACAR . . . accessed the TARGET WEBSITE."); *id.* at ¶ 26 ("My agency was provided with reliable information that a user had accessed the TARGET WEBSITE. Specifically, my agency learned that on May 2, 2019, IP address 24.194.90.108 accessed the TARGET WEBSITE."). In *Shacar*, HSI had more than the tip: they also learned that Mr. Shacar had "a juvenile criminal history including six counts of indecent assault and battery on a child under the age of 14." *Id.* at ¶ 42.

In *White*, the HSI agent also communicated the true meaning of the FLA's tip at various points in the affidavit. Ex. 7 (*White* Affidavit) at ¶ 7 ("There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE."); *see also id.* at ¶ 29 ("Affiant received and reviewed several files . . . available on the TARGET WEBSITE when the user connected to IP address 104.49.245.246 accessed the site."); *id.* at ¶ 36 ("IP address 104.49.245.246, which was used to access TARGET WEBSITE on April 11, 2019, was registered to AT&T."). Yet, as in Mr. Sanders's case, law enforcement appears not to have had any derogatory information about Mr. White, which is why only the paragraph specifically about the tip was phrased to suggest that the defendant had viewed illegal content on the target website, even though there was no such evidence. *Id.* at ¶ 28 ("HSI Special Agents received information from a[n] [FLA] known to the FBI . . . that [the] FLA determined that on April 11, 2019, IP address 104.49.245.246 was used to access online child sexual abuse and exploitation material' via a website that the FLA named and described as the TARGET WEBSITE.").

The cases that the defense has identified corroborate the true meaning of the FLA's tip, the FBI's and HSI's understanding that a bare tip that a user had accessed a website was insufficient for probable cause, and that this was a large-scale operation that could only generate so many IP address by use of a NIT that required law enforcement to rely on form affidavits and ECs to investigate such a large number of leads. At a minimum, the plethora of new evidence coming to light from the defense's own investigations warrants a *Franks* hearing for the government to produce what it has in its possession regarding its knowledge, prior to the execution of the search warrant, of the tip and the multi-national investigation that created the tip.

CONCLUSION

Mr. Sanders respectfully requests that the Court grant Mr. Sanders's previously filed Motions to Compel, order a hearing pursuant to *Franks v. Delaware,* 438 U.S. 154 (1978), suppress all evidence obtained pursuant to the invalid search warrant, and order a new trial pursuant to Fed. R. Crim. P. 33.

Respectfully submitted,

/s/
Jonathan Jeffress (#42884)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: jchong-smith@kaiserdillon.com

/s/
Nina J. Ginsberg (#19472)
DiMuroGinsberg, P.C.
1101 King Street, Suite 610
Alexandria, VA 22314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
Email: nginsberg@dimuro.com

/s/
H. Louis Sirkin (admitted *pro hac vice*)
Santen & Hughes
600 Vine Street, Suite 2700
Cincinnati, OH 45202
Telephone: (513) 721-4450
Facsimile: (513) 721-0109
Email: hls@santenhughes.com

Counsel for Defendant Zackary Ellis Sanders

CERTIFICATE OF SERVICE

I hereby certify that on this 21st day of March 2022, the foregoing was served electronically on the counsel of record through the US District Court for the Eastern District of Virginia Electronic Document Filing System (ECF) and the document is available on the ECF system.

/s/ Jonathan Jeffress
Jonathan Jeffress